

FILED

FEB 19 2020

UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY [Signature] DEP CLK

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)The Workspace of Edward Raff at Wahl Coates
Elementary School, 2200 East 5th Street, Greenville, NC
27858

Case No.

4:20-mj-1021

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC §§ 1028, 1028A, 1029, 1030, 1343, 2315	Aggravated Identity Theft, Access Device Fraud, Computer Fraud and Abuse, Wire Fraud and Sale or Receipt of Stolen Goods

The application is based on these facts:

See Attached Affidavit of Special Agent John Longmire.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Rule 4.1, the applicant appeared before me this day by reliable electronic means and swore to the contents of this application.

Applicant's signature

John Longmire, Special Agent, FBI

Printed name and title

Date: 2/19/2020City and state: Fayetteville, Greenville, North Carolina

Judge's signature

KIMBERLY A. SWANK, United States Magistrate Judge

Printed name and title

AFFIDAVIT

I, John Longmire, being duly sworn, depose and say as follows:

A. Identity and Experience of Affiant

1. AFFIANT, Special Agent John Longmire has been employed as a Special Agent with the Federal Bureau of Investigation ("FBI") for over thirteen years. I am assigned to the FBI's Washington Field Office Cyber Task Force.

2. Your affiant's official duties as a Special Agent include conducting and assisting in investigations into the activities of individuals and criminal groups responsible for cyber-crimes, including, cyber intrusions, online money laundering, criminal cryptocurrency usage, and criminal online forums. During my career, I have used a number of investigative techniques, including: (a) conducted, monitored, and reviewed physical and wire surveillance, including Title III wiretap investigations; (b) executed search warrants at locations where records of criminal activity have been found; (c) reviewed and analyzed numerous recorded conversations and other documentation of criminal activity; (d) debriefed cooperating defendants and confidential human sources; (e) monitored wiretapped conversations; (f) conducted surveillance of individuals engaged in various crimes; and (g) led and participated in search warrants and arrest warrants for various crimes.

3. Your affiant is the FBI "case agent" for this matter, which involves the unauthorized access of dozens of email accounts by a subject, Edward Raff, using various email accounts and access to usernames and passwords obtained from data breaches made available through subscriptions to various websites. Statements contained in this affidavit are based on direct personal knowledge derived from your affiant's investigation, information provided by other law enforcement officials, and information provided by non-law enforcement sources believed to be credible and to possess accurate information regarding the activities of the subject under investigation.

B. Purpose of Affidavit

4. The information in this affidavit is submitted for the limited purpose of supplying probable cause to support the application for a search warrant for the following locations controlled by Edward Raff ("Raff"):

- 2305 East 14th Street
Apartment 3
Greenville, NC 27858
with two specified vehicles if parked in the parking lot at that location
- 201-B South Elm Street
Greenville, NC 27858
with two specified vehicles if parked in the driveway at that location

Reviewed by: AUSAs SM and BR

- Workspace of Edward Raff at Wahl Coates Elementary School (including Raff's classroom, Raff's shared teacher office space, and any personal electronic storage locations of Raff on the network of Wahl Coates Elementary School)
2200 East 5th Street
Greenville, NC 27858
- The person of Edward Raff

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter. Rather, your affiant has set forth facts that are necessary to establish probable cause that the specific items to be seized, as set forth in Attachment B, constitute evidence of, and are fruits and instrumentality of, violations of Title 18, United States Code, §§ 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1029 (Access Device Fraud), 1030 (Computer Fraud and Abuse), 1343 (Wire Fraud), and 2315 (Sale or Receipt of Stolen Goods), hereafter referred to as the "subject violations."

C. Probable Cause

6. The United States is investigating the suspected unauthorized access of dozens of email accounts belonging to celebrities, journalists, athletes, and other individuals by a subject, Edward Raff, using various email accounts and access to usernames and passwords obtained from data breaches made available through subscriptions to various websites. The investigation concerns violations of 18 U.S.C. §§ 1028, 1028A, 1029, 1030, 1343, and 2315, as described above.

7. While conducting an internal review for business purposes, Google discovered information that it averred was harmful to its own business, operations, rights and property, and voluntarily provided that information to the FBI.

8. Google reported that in 2018 and 2019, a Google subscriber (Raff) used Internet Protocol (IP) addresses that resolve to the District of Columbia public wi-fi to access or attempt to access the Google accounts of between sixty and eighty celebrities, journalists, athletes, and others. One of Raff's methods involved creating fraudulent accounts designed to mimic accounts owned by the victims, for example by creating accounts with one or two letters different from the victim account, or by using an easily glossed over misspelling. The fraudulent accounts were used in attempts to compromise the victims' actual accounts.

9. According to business records provided by Google, several email accounts used in this scheme are controlled by Raff, including edward.b.raff19@gmail.com, volmon68@gmail.com, volrnon@aol.com, and rick.rnvey@gmail.com. The subscriber records for the edward.b.raff19@gmail.com account includes Raff's true name and billing information. The recovery email address for edward.b.raff19@gmail.com is volmon68@gmail.com. Subscriber records for volmon68@gmail.com include a recovery

email address of volrnon@aol.com. Additionally, edward.b.raff19@gmail.com is listed as the recovery email address for rick.rncvey@gmail.com.

10. Business records provided by Google also showed that edward.b.raff19@gmail.com, volmon68@gmail.com, and rick.rncvey@gmail.com were linked by cookies to a majority, if not all, of the victim accounts.¹

11. The email address rick.rncvey@gmail.com created by Raff uses a “r” and an “n” together to trick the reader into reading an “m.” This email address is likely made to look like it is used by “RM,” chief executive officer of a financial technology company. Raff also did this with volrnon@aol.com to make it look similar to volmon68@gmail.com. As noted below, Raff used volmon68@gmail.com to receive forwarded emails that contained compromising images.

12. In the course of the investigation, the FBI obtained, pursuant to legal process, IP logs for many of the compromised victim accounts. On multiple occasions, victim accounts and accounts maintained by Raff were accessed by the same IP on the same date within relatively short time frames. The following chart illustrates examples:

Date	Time Period	IP Address	Accounts Accessed
11/26/18	5:57 am to 1:55 pm UTC	174.255.198.30 ²	volrnon@aol.com and two victim accounts
11/26/18	3:18 pm to 10:44 pm UTC	164.82.84.22 ³	volrnon@aol.com, Raff's PayPal account, and three victim accounts
1/30-1/31/19	10:37 pm to 12:11 am UTC	164.82.84.22	volrnon@aol.com, Raff's PayPal account, and three victim accounts
2/14/19	7:24 pm to 7:29 pm UTC	164.82.84.22	volrnon@aol.com and three victim accounts
4/319	6:17 pm to 10:59 pm UTC	164.82.84.21	volmon68@gmail.com, Raff's PayPal account, and two victim accounts

¹As described below, basically, a “cookie” is a small file containing a string of characters that a website attempts to place onto a user’s computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to the website/relevant internet services provider. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by various internet services providers may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a particular internet services provider account and determine the scope of the criminal activity.

² 174.255.198.30 is an IP address that resolves to Verizon Wireless. Subscriber records show that Verizon Wireless resold the IP to TracFone Wireless, which is a prepaid cellular service that does not require the customer’s identity.

³ IP addresses 164.82.84.20 through 164.82.84.22 resolve to the DC Public Wifi.

Date	Time Period	IP Address	Accounts Accessed
5/8/19	5:47 pm to 9:24 pm UTC	164.82.84.20	edward.b.raff19@gmail.com and one victim account
5/13/19	3:28 pm to 8:54 pm UTC	164.82.84.20	Raff's PayPal account and three victim accounts
6/18/19	8:25 pm to 10:35 pm UTC	164.82.84.22	volmon@aol.com, volmon68@gmail.com, Raff's PayPal account, and two victim accounts
7/30/19	2:41 pm to 6:47 pm UTC	164.82.84.22	volmon@aol.com, Raff's PayPal account, and two victim accounts

13. Your affiant interviewed several victims, all of whom confirmed that they did not access their accounts during the relevant timeframe, nor have they accessed accounts via the D.C. public wifi. In fact, one victim reported that he/she had not accessed his/her account since 2014.

14. Weleakinfo.com was, until its domain name was seized by the FBI in January 2020, a website that provided its users a search engine to review and obtain the personal information illegally obtained in over 10,000 data breaches containing over 12 billion indexed records – including, for example, names, email addresses, usernames, phone numbers, and passwords for online accounts. The website sold subscriptions so that any user could access the results of these data breaches, with subscriptions providing unlimited searches and access during the subscription period (one day, one week, one month, or three months). According to records obtained from PayPal, security@wli.design is the username for weleakinfo.com's PayPal account.

15. Between 8:52 p.m. UTC and 10:11 p.m. UTC, on July 10, 2019, IP address 164.82.84.21 accessed Raff's PayPal account, edward.b.raff19@gmail.com, and four victim accounts, one of which belonged to WAD. Within 28 seconds during this timeframe, Raff logged into his edward.b.raff19@gmail.com PayPal account, sent a payment to security@wli.design, received an email from service@paypal.com, and received an email from no-reply@weleakinfo.com. Within seven minutes, victim accounts were being accessed from the same aforementioned IP address.

16. Similarly, between 7:22 p.m. UTC and 9:55 p.m. UTC on July 12, 2019, the IP address 164.82.84.22 was used to access Raff's email account volmon68@gmail.com, Raff's PayPal account edward.b.raff19@gmail.com, as well as six victim accounts, two of which belonged to MNH and CAD. Within 13 seconds during this timeframe, Raff logged into his edward.b.raff19@gmail.com PayPal account, sent a payment to security@wli.design, received an email from service@paypal.com, and received an email from no-reply@weleakinfo.com confirming receipt of this payment. Within 15 minutes, victim accounts and Raff's email account, volmon68@gmail.com, were being accessed simultaneously from the same aforementioned IP address. MNH and CAJ both independently confirmed that neither accessed his/her account during that timeframe. Neither MNH nor CAJ have ever been to

Washington, D.C. nor accessed the D.C. public wifi. CAJ has not accessed his/her account since 2012 or 2013. MNH has not accessed his/her account since 2016.

17. Based on this information, there is probable cause to conclude that Raff purchased subscriptions to weleakinfo.com, conducted searches of the data breaches, and obtained information allowing Raff to access the victim accounts without authorization.

18. In the course of the investigation, the FBI obtained, pursuant to legal process, email content and other records for Raff's email accounts: edward.b.raff19@gmail.com, volmon68@gmail.com and rick.mcvey@gmail.com.

19. Raff's volmon68@gmail.com email account contained several forwarded emails received from Raff's other email account, volrnon@aol.com, which were forwarded from a victim email account, g****x@aol.com. The emails contained images ("selfies") of a female individual in various states of undress ranging from bathing suits or lingerie to completely nude.

20. Raff's volmon68@gmail.com email account also contained several forwarded emails received from a victim email account, l****r@aol.com. These emails similarly contained selfies of a female individual in various states of undress ranging from underwear to completely nude. Additional forwarded emails from this victim account contained photos of a male individual receiving oral sex from a female individual.

21. There is probable cause to conclude, based on your affiant's training, experience, and the evidence gathered to date, that the account holders of the g****x@aol.com account and l****r@aol.com account are victims in this scheme and did not authorize the forwarding of emails to Raff's volmon68@gmail.com or volrnon@aol.com email accounts.

22. For Raff's volmon68@gmail.com email account, records from Google revealed that Raff lists the name visible to email recipients as Kenny Chesney. In email content, Raff claims to be Kenny Chesney, the country music singer, in order to exchange sexual emails with KK. Using this ruse, Raff received attachments from KK that include images of a female in various states of undress ranging from lingerie to completely nude and videos of a female engaged in masturbation. For Raff's volrnon@aol.com email account, Raff lists the name visible to email recipients as Bobby Crouton, an alias Kenny Chesney used earlier in his career. Raff's edward.b.raff19@gmail.com account's search history contained several searches regarding Kenny Chesney.

23. Raff's edward.b.raff19@gmail.com account contained Raff's internet search history. On May 8, 2019, around 5:42 p.m. Raff searched for "university of Arizona email" and visited "CatMail Student Email | Information Technology | University of Arizona" a few seconds later. Approximately four minutes later, Raff was accessing MNH's arizona.edu email account as described earlier. Approximately five minutes after accessing MNH's email account, at 6:01 p.m. UTC, Raff performed searches on BH who has the same last name as MNH. Raff then visited BH's LinkedIn profile. Raff's search history also includes searching for several other University email systems and several other individual's names.

24. Raff also searched for and visited the website leakedsource.ru, which is a service that sends email notifications about new breaches and offers a database of information from data breaches.

25. Raff also searched for "iphone backup extractor" and visited www.iphonebackupextractor.com, which is used to obtain data, images, videos, and other files out of an iPhone backup. Reincubate is the company that created iphonebackupextractor.com. Through Raff's PayPal account, edward.b.raff19@gmail.com, Raff purchased nine subscriptions for iphonebackupextractor.com, which can each be used on five Apple iCloud accounts for a total of 45 accounts. Raff had several email conversations with Reincubate customer care representatives in Raff's true name, where Raff inquired how many account downloads he has left on his iphonebackupextractor.com subscription. Raff also complained to Reincubate that he was unable to search or copy and paste messages he extracted from iPhone backups. CAJ and WAD both stated they had issues with the security of their iCloud accounts.

26. Raff's search history also included, "how to decipher hash," "decipher hashed password," "buy bitcoin with prepaid card," "sms verification online," and several questions indicating Raff was trying to figure out the answers to victim's personal security questions.

27. Raff's volmon68@gmail.com account's Google Drive had a deleted file, which contained a text message string of 55,021 messages between two victims. This file was generated by Reincubate's iPhone Backup Extractor.

28. Raff's edward.b.raff19@gmail.com email account contained two draft emails of note. One contained Raff's username and password to weleakinfo.com and leakedsource.ru, both of which are websites that allow users to obtain, without the authorization of the account holders, username and password combinations to various online accounts. The other draft email contained over 400 pages of email addresses and usernames with associated passwords. L***r@aol.com and its associated password were contained the second draft email.

29. In the course of the investigation, the FBI obtained, pursuant to legal process, PayPal records for Raff. These records showed from December 13, 2017 to August 7, 2019, Raff purchased at least 46 subscriptions from weleakinfo.com. The subscriptions Raff purchased ranged from one day to one month.

30. Based on this information, there is probable cause to conclude that Raff purchased subscriptions to weleakinfo.com, then conducted searches of the data breaches hosted by weleakinfo.com, and obtained username and password information for victim accounts from weleakinfo.com—allowing Raff to access the victim accounts without authorization. There is also probable cause to conclude that Raff created his 400 page email (containing means of identification such as emails, usernames, and passwords, and other information useful for identifying specific individuals) through using his subscriptions to weleakinfo.com to conduct searches of the data breaches.

31. Based on a search of Accurant's Advanced Person Search, Raff currently resides at 2305 East 14th Street, Apartment 3, Greenville, NC 27858. As of October 31, 2019, the landlord for the premises reported that Raff continued to lease that apartment. Additionally, Raff lists this address on his PayPal account and Bank of America account.

32. Raff is currently employed by Wahl Coates Elementary School, 2200 East 5th Street, Greenville, NC 27858. Based on records received, pursuant to legal process, Raff accessed his PayPal and Bank of America accounts with his mobile phone through a wireless application protocol from an IP addresses that resolve to the North Carolina Research and Education Network (NCREN). NCREN provides broadband communications technology services and support to K-12 school districts across North Carolina. Based on this information, there is probable cause to conclude that Raff used the wireless network at Wahl Coates Elementary School in order to access his accounts.

33. Raff's workspace at the Wahl Coates Elementary School includes the following: classroom A3 and a shared teacher office space. Based on the investigation, law enforcement has learned that Raff does have access to, and does store files on, the computer network of the Wahl Coates Elementary School.

34. Based on surveillance during the afternoon of January 29, 2020, Raff was seen traveling with a female companion, KBN, from Wahl Coates Elementary School to KBN's residence, 201-B South Elm Street, Greenville, NC 27858 in KBN's vehicle, a gray Ford Explorer XLT with North Carolina license Plate OBX89058. Raff's vehicle, a white Nissan Frontier with North Carolina license plate HAW 5880, was also located at KBN's residence. On February 4, 2020, at approximately 4:04 p.m., Raff and KBN were seen leaving Wahl Coates Elementary School and traveling to KBN's residence in Raff's vehicle. On February 5, 2020 at approximately 7:17 a.m., Raff and KBN were seen leaving KBN's residence and traveling to Wahl Coates Elementary School in Raff's vehicle. On multiple occasions, Raff was seen carrying a backpack, which likely stores Raff's electronic devices.

35. Additionally, surveillance on November 25, 2019 observed Raff arriving at KBN's residence at 3:20 p.m. after leaving Wahl Coates Elementary School at 3:15 p.m.

36. After the above-referenced observations, Raff purchased a new vehicle, a blue Chevrolet Equinox with North Carolina license plate HAW 5880 – that is, Raff, transferred the tag from his prior vehicle (the Nissan Frontier) to the blue Chevrolet Equinox. Surveillance on February 12, 2020 observed Raff leaving KBN's residence at 7:20 a.m. and driving to Wahl Coates Elementary School in the Chevrolet Equinox.

37. Authority to search is sought for both identified vehicles if they are parked in the parking lot of the premises described above. On February 14, 2020, surveillance observed Raff using a mobile phone while driving the Chevrolet Equinox from Wahl Coates Elementary School to KBN's residence. In my training and experience, subjects often travel with their portable electronic devices, as Raff was observed doing, such as cell phones, laptops, and tablet computers, and such devices may be left in cars at times.

38. Authority to search is sought for the person and property of Raff, a white male, who (according to public records, such as his driver's license) is approximately 6 feet, 1 inch tall, and weighs about 185 pounds. Raff has a date of birth of 5/19/1990, and social security number ending in 6224. The proposed warrant authorizes to search of the person of Edward Raff, including any digital devices on his person or within his immediate wingspan, such as devices in the passenger compartment of a vehicle he exits.

39. Based on my training and experience, cybercrime subjects are known to keep their devices (computers and smart phones) at their residence and place of employment, when not on or about their person. Subjects are also known to have their smart phones with them or near them when staying somewhere that is not their residence. Subjects are also known to use their computers at their place of employment in order to advance their scheme, and in fact, as described above, Raff did use one of his devices at his place of employment.

40. Based on my training and experience, I know that persons engaged in cyber-enabled offense schemes like the one described here will use computers (including smartphones) to engage in those activities. Evidence of these crimes will typically be retained on a computer for a long time, particularly with the enormous – and growing – amounts of data storage space available on computers. Even when a person obtains and uses a new computer or smartphone, data contained on an older computer or smartphone will typically be transferred to the new computer, ensuring information important to the user is maintained, including historical data, login/password credentials, and even deleted data that has not yet been overwritten. In addition, historical data is often transferred to external data storage media and external cloud storage accounts on a frequent basis, typically through the creation of data backups. With virtually unlimited data storage space available at a very low cost, it has been my experience that users usually retain all of their historical data, including previous backups.

41. Based on my training, experience, and knowledge of this investigation, I expect that a search of the premises will reveal evidence of Raff's criminal activity as listed in Attachment B. The investigation has shown that Raff resides at the East 14th Street and South Elm Street premises, and works at the Wahl Coates Elementary School premises, and is responsible for the offenses described above. Moreover, there is probable cause to believe that Raff keeps at least some of his digital devices (which are likely to contain evidence of these offenses) on or about his person, as most people do, particularly including cyber-criminals engaged in offenses of this nature. In my training, experience, and knowledge of this investigation, there is probable cause to believe that Raff has kept electronic and physical evidence of his schemes, and that that evidence will be located in the various premises.

42. For each of the locations to be searched, the property to be searched includes laptop computers, mobile phones, tablets, and/or other digital devices or electronic devices owned, used, or controlled by Raff, as described in more detail in Attachment B.

D. Computers, Electronic/Magnetic Storage, and Forensic Analysis

43. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the

premises, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the premises, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

- A. Individuals who engage in criminal activity, including identity theft, aggravated identity theft, and computer fraud, and related offenses, use digital devices to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social media accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and (4) store stolen data for future exploitation.
- B. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.
- C. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on

the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

44. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

- A. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized

tools and a controlled laboratory environment, and also can require substantial time.

- B. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.
- C. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.
- D. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- E. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user’s intent and the identity of the user.
- F. I know that when an individual uses a digital device to access other computers without authorization, the individual’s device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

E. Methods to be used to search digital devices

45. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

Reviewed by: AUSAs SM and BR

- A. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.
- B. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.
- C. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.
- D. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital

devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

- E. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.
- F. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

46. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Therefore,

in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

- A. Upon securing the premises, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the premises. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.
- B. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.
- C. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

F. Biometric access to devices

47. This warrant permits law enforcement agents to obtain from the person of Edward Raff (but not any other individuals present at the premises at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)’ physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows.

48. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

49. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

50. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

51. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

52. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

53. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data

contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

54. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

55. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the premises; (2) hold the Device(s) found at the premises in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the premises in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

56. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

G. Authorization to search at any time of the day or night

57. Law enforcement personnel will commence the execution of this search and seizure warrant upon the premises during daytime hours (between 6:00 a.m. and 10:00 p.m.), including but not limited to after school hours to limit insofar as possible any disruption of school operations. It is anticipated that law enforcement personnel will attempt to image or copy digital information from certain servers on the premises, rather than remove those servers from the premises. Such onsite imaging or copying will minimize disruptions to the use of those servers.

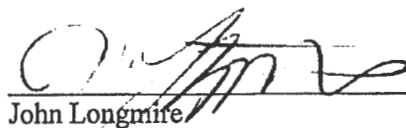
58. From my training and experience, I know that imaging or copying information from servers on the premises can be substantially delayed by various factors which cannot be ascertained or sometimes even anticipated until the actual execution of the warrant. There may, for example, be no system administrator available, willing, or able to assist law enforcement personnel to narrow the search by identifying the virtual or dedicated server(s) on the premises, or the server folders, containing information within the scope of the warrant. There may be terabytes or even petabytes of information to be copied. The network architecture of the servers on the premises or the configuration of the server hardware may affect and delay data transfer speeds. Data encryption and password protections may also significantly delay imaging or copying as law enforcement personnel seek to identify necessary passwords without which imaging or copying on the premises would likely be unachievable. Under some circumstances, data downloads can be interrupted by network or hardware malfunctions or other network or hardware attributes which often necessitates restarting the data downloads from the beginning.

59. For all of the foregoing reasons, I respectfully submit that good cause exists, pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), for authorization to execute the search warrant at any time of the day or night. Law enforcement personnel will commence executing the warrant between 6:00 a.m. and 10:00 p.m. However, given the myriad factors that that may prevent completion of the search and seizure by 10:00 p.m., including those described above, I request authorization to continue the warrant execution past 10:00 p.m., if necessary, until completion of the warrant execution. Suspending the execution at 10:00 p.m. until 6:00 a.m. could compromise data downloads in progress, render stored data subject to alteration or deletion, require securing the premises during the intervening hours, and prolong the disruption of access to, and use of, the premises and the digital devices being searched.

H. Conclusion

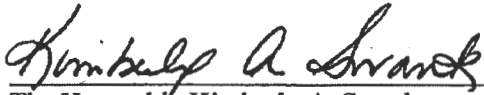
60. Based on the foregoing, I submit there is probable cause to believe violations of 18 U.S.C. §§ 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1029 (Access Device Fraud), 1030 (Computer Fraud and Abuse), 1343 (Wire Fraud), and 2315 (Sale or Receipt of Stolen Goods) have occurred and that evidence of the aforementioned violations of law will be present at 2305 East 14th Street, Apartment 3, Greenville, NC 27858 (with two specified vehicles if parked in the parking lot at that location); 201-B South Elm Street, Greenville, NC 27858 (with two specified vehicles if parked in the driveway at that location); the workspace of Edward Raff at Wahl Coates Elementary School (including Raff's classroom, Raff's shared teacher

office space, and any personal electronic storage locations of Raff on the network of Wahl Coates Elementary School), 2200 East 5th Street, Greenville, NC 27858; and the person of Edward Raff. Therefore, this affidavit seeks a search warrant to be issued for the subject locations.



John Longmire
Special Agent
Federal Bureau of Investigation

Pursuant to Federal Rule of Criminal Procedure 4.1, on this 19th day of February, 2020, Special Agent John Longmire appeared before me via reliable electronic means, was placed under oath and attested to the contents of this affidavit in support of this application for a Search Warrant.



The Honorable Kimberly A. Swank
United States Magistrate Judge

Reviewed by: AUSAs SM and BR

ATTACHMENT A
LOCATION TO BE SEARCHED

The location to be searched is *the workspace of Edward Raff at Wahl Coates Elementary School, 2200 East 5th Street, Greenville, NC 27858* – that is, specifically, Raff’s classroom, identified as Classroom A3, and Raff’s shared teacher office space, and any personal electronic storage locations of Raff on the network of Wahl Coates Elementary School.

A photo of the location is included below:



ATTACHMENT B
ITEMS TO BE SEIZED

The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of Title 18, United States Code, §§ 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1029 (Access Device Fraud), 1030 (Computer Fraud and Abuse), 1343 (Wire Fraud), and 2315 (Sale or Receipt of Stolen Goods), as described in the search warrant affidavit, including, but not limited to:

1. Records and information relating to a scheme (and/or conspiracy) to defraud victims of their Personal Identifying Information (PII), account usernames and passwords, videos and images, or any other thing of value, or relating to Edward Raff's efforts to otherwise obtain the same information about victims;
2. Records and information relating to unauthorized access of any victim's accounts;
3. Records and information relating to WeLeakInfo or any other online site used to obtain PII or account user names and passwords;
4. Records and information relating to any steps taken to obfuscate a user's online identity when accessing the online accounts of others, such as accessing the D.C. public wifi or a VPN;
5. Records and information relating to the identity or location of perpetrators, aiders and abettors, coconspirators, and accessories after the fact;
6. Records and information relating to malicious software;
7. Records and information that constitute evidence of the state of mind of Edward Raff, e.g., intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation;
8. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with Edward Raff about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;
9. Records and information that constitute evidence of use, control, ownership, or occupancy of the premises and things therein;
10. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with Edward Raff about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

11. Digital devices used in the commission of or to facilitate the above described offenses, including digital devices used to store the proceeds or digital goods obtained through those offenses;
12. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the "Device(s)":
 - a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
 - b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;
 - d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
 - e. evidence of the times the Device(s) was used;
 - f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
 - g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
 - h. records of or information about Internet Protocol addresses used by the Device(s);
 - i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses
13. During the execution of the search, law enforcement personnel are also specifically authorized to obtain from Edward Raff (but not any other individuals present at the premises at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor or any other security feature requiring biometric recognition of:
 - a. any of the Device(s) found at the premises,
 - b. where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or

instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

- c. for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.
 - d. While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.
14. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
15. "Digital device," as used herein, includes the following three terms and their respective definitions:
- a. A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. See 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.
 - b. "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.
 - c. "Computer hardware" means all equipment that can receive, capture, collect,

analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

16. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.
17. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.
18. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

19. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
20. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
21. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
22. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
23. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.
24. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

25. A “router” often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.
26. “Domain Name” means the common, easy-to-remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.
27. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.
28. “Peer to Peer file sharing” (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user’s computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.
29. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file’s hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.
30. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.
31. “VPN” means a virtual private network. A VPN extends a private network across public

networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

32. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.
33. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.